PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-179726
(43)Date of publication of application : 11.07.1997

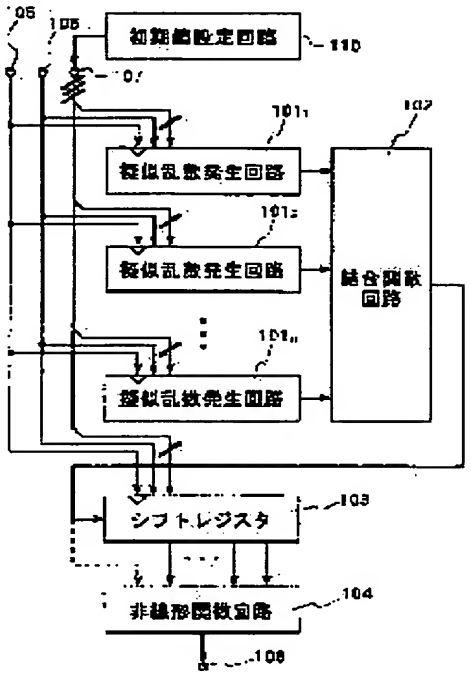
(51)Int.Cl. G06F 7/58

(21)Application number : 07-336920
(22)Date of filing : 25.12.1995

(71)Applicant : NEC CORP
(72)Inventor : SHIMADA MICHIO

(54) PSEUDO RANDOM NUMBER GENERATOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a pseudo random number generator suitable for stream ciphers by generating a nonlinear large pseudo random number sequence by a pseudo random number generation circuit.
SOLUTION: An initial state setting circuit 110 is connected so as to set the bit sequence of an initial state to respective pseudo random number generation circuits 1011-101n and a shift register 103. In the case of generating pseudo random numbers, the initial state of the pseudo random number generation circuits 1011-101n and the shift register 103 is supplied to an input terminal 107 by an initial value setting circuit 110. Then, '0' is supplied to the input terminal 106 and one control pulse is inputted to the input terminal 105. As a result, the initial state is set to the pseudo random number generation circuits 1011-101n, and the shift register 103. Then, when '1' is supplied to the input terminal 106, the pseudo random numbers are obtained bit by bit from an output terminal 108 every time one control pulse is inputted to the input terminal 105 thereafter.



LEGAL STATUS

[Date of request for examination] 25.12.1995
[Date of sending the examiner's decision of rejection] 18.08.1998
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－179726

(43)公開日　平成９年(1997)７月11日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　7/58			Ｇ０６Ｆ　7/58	Ａ

審査請求　有　　請求項の数６　ＯＬ　（全 10 頁）

(21)出願番号　特願平7－336920

(22)出願日　平成７年(1995)12月25日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝五丁目７番１号　日本電気株式会社内

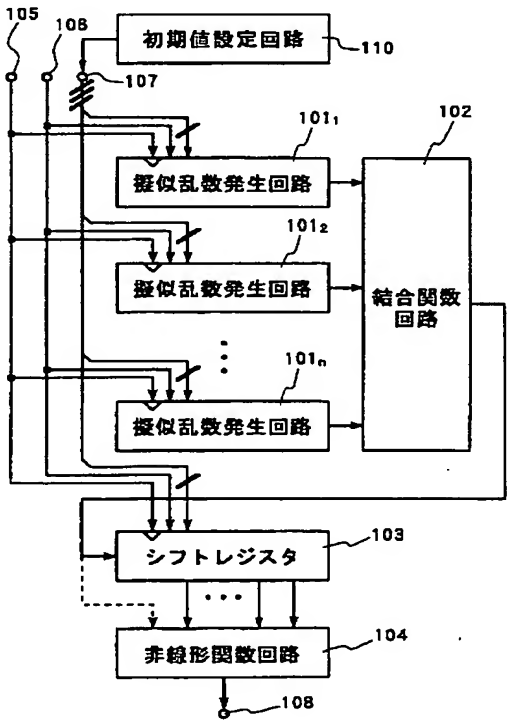
(74)代理人　弁理士　若林　忠

(54)【発明の名称】　擬似乱数発生装置

(57)【要約】

【課題】装置規模が小さくてすみ、線形フィードバック・シフトレジスタのみからなる少数の擬似乱数発生回路によって非線形性の大きな擬似乱数系列を発生でき、ストリーム暗号に適した擬似乱数発生装置を提供する。

【解決手段】ｎ個の擬似乱数発生回路１０１$_1$～１０１$_n$と、これらｎ個の擬似乱数発生回路１０１$_1$～１０１$_n$の出力を非線形結合してその結果を出力する結合関数回路１０２と、結合関数回路１０２の出力がシフト入力として入力するシフトレジスタ１０３と、シフトレジスタ１０３の内部状態のうち予め定められた複数のビットの非線形結合を計算する非線形関数回路１０４とを設け、非線形関数回路１０４での計算結果が擬似乱数を表わすビットストリームとして出力端子１０８から出力されるようにする。



1

【特許請求の範囲】

【請求項１】　同一のクロックが入力し相互に同期して動作する複数の擬似乱数発生回路と、
前記各擬似乱数発生回路の出力を非線形関数で結合して出力する結合関数回路と、
前記クロックに同期して記憶内容を一端から他端に向う方向に１ビットずつシフトするとともに前記結合関数回路の出力を前記一端に記憶するシフトレジスタと、
前記シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路とを有し、
前記クロックに同期して前記非線形関数回路より擬似乱数を出力することを特徴とする擬似乱数発生装置。

【請求項２】　同一のクロックが入力し相互に同期して動作する複数の擬似乱数発生回路と、
前記各擬似乱数発生回路の出力を非線形関数で結合して出力する結合関数回路と、
シフトレジスタと、
前記シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路と、
前記結合関数回路の出力と前記非線形関数回路の出力との排他的論理和を計算して出力する排他的論理和回路とを有し、
前記シフトレジスタは、前記クロックに同期して記憶内容を一端から他端に向う方向に１ビットずつシフトするとともに前記排他的論理和回路の出力を前記一端に記憶し、擬似乱数が前記クロックに同期して前記非線形関数回路より出力されることを特徴とする擬似乱数発生装置。

【請求項３】　入力するクロックに同期して動作する単一の擬似乱数発生回路と、
シフトレジスタと、
前記シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路と、
前記擬似乱数発生回路の出力と前記非線形関数回路の出力との排他的論理和を計算して出力する排他的論理和回路とを有し、
前記シフトレジスタは、前記クロックに同期して記憶内容を一端から他端に向う方向に１ビットずつシフトするとともに前記排他的論理和回路の出力を前記一端に記憶し、擬似乱数が前記クロックに同期して前記非線形関数回路より出力されることを特徴とする擬似乱数発生装置。

【請求項４】　前記擬似乱数発生回路と前記シフトレジスタに初期値を設定する初期値設定回路をさらに有する請求項１乃至３いずれか１項に記載の擬似乱数発生装置。

【請求項５】　前記結合関数回路の出力も前記非線形関数回路に入力し、前記非線形関数回路が前記シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値と前記結合関数回路の出力とを非線形結合して出力する請求項１または２に記載の擬似乱数発生装置。

【請求項６】　前記擬似乱数発生回路が線形フィードバック・シフトレジスタである請求項１乃至５いずれか１項に記載の擬似乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、擬似乱数を発生する擬似乱数発生装置に関し、特に、複数の擬似乱数発生回路を有しこれら擬似乱数発生回路の出力を非線形結合して擬似乱数を出力する擬似乱数発生装置に関する。

【０００２】

【従来の技術】通信システムや計算機システムにおいては、許可されていない者が不正に情報を取得することなどを防止するために、情報に擬似乱数を排他的論理和で加算して暗号に変換したり、暗号に擬似乱数を排他的論理和で加算して元の情報を復元したりするストリーム暗号装置などが使用される。

【０００３】情報への不正なアクセスを防ぐための暗号化に使用される擬似乱数は、以下に説明するように、非線形性が高いことが必須であり、そのため、暗号化に使用される擬似乱数の発生方法として、結合関数と呼ばれる非線形関数によって複数の擬似乱数発生回路の出力を非線形結合して非線形性のより高い擬似乱数を生成する方法が、従来より広く知られている。以下、擬似乱数発生回路とは、線形フィードバック・シフトレジスタなど、擬似乱数を与える基本的な回路のことを指し、擬似乱数発生装置とは、１または複数の擬似乱数発生回路を含んでより非線形性の高い擬似乱数を発生する装置のことを言う。

【０００４】ここで非線形結合とは、線形結合ではない結合のことである。ビット$x_1,\cdots,x_n,\cdots$の線形結合とは、$y=x_1+x_2+\cdots+x_n$や$y=x_1+x_2+\cdots+x_{n+1}$など、排他的論理和"＋"だけを使ってビットｙを与えることである。したがって、ビット$x_1,\cdots,x_n,\cdots$の非線形結合とは、$y=x_1*x_2+x_2*x_3+\cdots+x_n*x_1$など、論理積"＊"と排他的論理和"＋"の両方（否定論理を含んでもよい）を使ってビットｙを与えることであり、ｙを与える式をどのように変形しても線形結合に帰着しないようなものである。また、非線形結合の非線形性とは、ｙを与える式の次数のことであり、式の次数が大きいほど非線形性が高いとされる。なお、非線形関数の入力（結合されるべき擬似乱数発生回路の数）を増やすほど、非線形性の高い非線形結合が実現可能になる。

【０００５】図４は、従来の擬似乱数発生装置の一例の構成を示す機能ブロック図である。この擬似乱数発生装置はｎ個の擬似乱数発生回路401_1～401_nと、これらｎ個の擬似乱数発生回路401_1～401_nの出力を非

線形結合して擬似乱数を出力端子４０８から出力する結合関数回路４０２と、制御パルス（クロック）が入力する入力端子４０５と、モード制御用の入力端子４０６と、初期状態と呼ばれるビット系列を入力するための入力端子４０７とから構成されている。ｎ個の擬似乱数発生回路401_1～401_nは、いずれも、入力端子４０５～４０７に接続しており、入力端子４０６に"０"が供給されている時に入力端子４０５に制御パルスが入力された場合には、入力端子４０７から供給される初期状態を取り込んで内部状態として保持し、入力端子４０６に"１"が供給されている場合には、入力端子４０５に制御パルスが１個入力されるごとに擬似乱数を出力するように構成されている。なお、擬似乱数発生回路401_1～401_nには、一般に、それぞれ異なる初期状態が供給される。

【０００６】図４の擬似乱数発生装置を用いて擬似乱数を発生させる場合には、まず、入力端子４０７に初期状態を供給し、次に、入力端子４０６に"０"を供給して、入力端子４０５に制御パルスを１個入力する。そして、入力端子４０６に"１"を供給する。するとそれ以降は、入力端子４０５に制御パルスを１個入力するごとに、各擬似乱数発生回路401_1～401_nの出力を結合関数回路４０２によって非線形結合して得られた擬似乱数が、出力端子４０８から得られる。

【０００７】しかしながら、図４に示す擬似乱数発生装置は、しばしば、各擬似乱数発生回路401_1～401_nに設定された初期状態がコリレーション・アタックと呼ばれる解読方法によって推定されてしまい、その結果、暗号の不正な解読を許してしまうという問題点がある。すなわち、ある擬似乱数発生回路401_j（$1 \leq j \leq n$）の出力で条件付けたときの結合関数回路４０２の出力の条件付き確率分布が一様でない場合には、その擬似乱数発生回路401_jと等価な擬似乱数系列発生回路を想定し、この擬似乱数系列発生回路の出力系列と結合関数回路４０２の出力系列との相関が最大になるようにその擬似乱数系列発生回路の初期状態を求めることで、擬似乱数発生回路401_jに与えられた初期状態を知ることができる。このような性質があると、ストリーム暗号の擬似乱数発生装置としては使えない。なお、コリレーション・アタックに関しては、R. A. Rueppel（ルエペル）著、"Analysis and Design of Stream Ciphers（アナリシス・アンド・デザイン・オブ・ストリーム・サイファーズ）", Springer-Verlag（スプリンガー・ヴァーラグ）社、１９８６年の第９２頁から第１４１頁にその詳しい解説がある。

【０００８】そこで本発明者は、コリレーション・アタックによる解読を防ぐために、特開平７－１０４９７６号公報において、結合関数回路が出力するビットストリームをそのまま擬似乱数として使うのではなく、結合関数回路の出力を畳み込んで得られるビットストリームを

擬似乱数として用いる擬似乱数発生装置を提案した。そのようにすれば、ある擬似乱数発生回路の出力で条件付けたときの擬似乱数の条件付き確率分布がほぼ一様になり、コリレーション・アタックが困難になる。

【０００９】図５は、コリレーション・アタック対策を施した従来の擬似乱数発生装置の一例を示す機能ブロック図である。この擬似乱数発生装置は、図４に示す擬似乱数発生装置において、結合関数回路４０２と出力端子４０８との間に、シフトレジスタ４１０と排他的論理和回路４１１を挿入した構成である。シフトレジスタ４１０は、入力端子４０５～４０７にも接続しており、入力端子４０６に"０"が供給されている時に入力端子４０５に制御パルスが入力すると、入力端子５０７から供給されている初期状態と呼ばれるビット系列を内部状態として保持し、入力端子５０６に"１"が供給されている場合には、入力端子５０５に制御パルスが１個入力されるごとに、内部状態を１ビットだけ右にシフトし、左端のビットに結合関数回路４０２の出力を保持するように構成されている。また、排他的論理和回路４１１は、シフトレジスタ４１０の内部状態のうち予め決められた複数のビットの線形結合を計算するものであり、その計算結果が擬似乱数として出力端子４０８から出力される。なお、図示点線で示されるように、結合関数回路４０２の出力も排他的論理和回路４１１に入力するようにしてもよい。

【００１０】図５に示す擬似乱数発生装置を用いて擬似乱数を発生させる場合には、まず、入力端子４０７に初期状態を供給し、次いで入力端子４０６に"０"を供給して、入力端子４０５に制御パルスを１個入力する。そして、入力端子４０６に"１"を供給する。するとそれ以降は、入力端子４０５に制御パルスを１個入力するごとに、出力端子４０８から擬似乱数が得られる。

【００１１】図６は、シフトレジスタ４１０の内部構成を示す回路図である。このシフトレジスタ４１０はｍ段構成であり、クロック入力端子４１５と、モード切り換え信号入力端子４１６と、このシフトレジスタ４１０に内部状態を設定するための内部状態入力端子４１７と、このシフトレジスタ４１０の内部状態を出力するための内部状態出力端子４１８と、シフト入力端子４１９と、モード切り換え信号入力端子４１６に入力した信号に応じて選択動作を行うｍ個の２入力セレクタ421_1～421_mと、クロック入力端子４１５に入力した信号をクロックとしセレクタ421_1～421_mの出力をそれぞれ入力とするｍ個のＤ型フリップフロップ422_1～422_mによって構成されている。なお、Ｄ型フリップフロップ422_1～422_mの出力系列のことをこのシフトレジスタ４１０の内部状態という。図５に示される状態では、このシフトレジスタのクロック入力端子４１５は入力端子４０５に接続し、モード切り換え信号入力端子４１６は入力端子４０６に接続し、内部状態入力端子４１

７は入力端子４０７に接続し、シフト入力端子４１９は結合関数回路４０２の出力に接続している。

【００１２】図示左端のセレクタ421_1には、シフト入力端子４１９を介して結合関数回路４０２（図５参照）が入力するとともに、内部状態入力端子４１７から入力した内部状態のうちの１ビットが入力する。その他のセレクタ421_j（Ｊ＝２,…,ｍ）には、それぞれ、Ｄ型フリップフロップ421_{j-1}の出力と、内部状態入力端子４１７から入力した内部状態のうちのそれぞれに固有の１ビットとが入力する。そして、各セレクタ421_1～421_mは、モード切り換え信号入力端子４１６から"０"が供給されている時に、それぞれ内部状態入力端子４１７から供給されるビットを選択して出力し、モード切り換え信号入力端子４１６から"１"が供給されているときには、シフト入力端子４１９や前段のＤ型フリップフロップ422_1～422_{m-1}から入力する信号を選択して出力する。各Ｄ型フロップフロップ422_1～422_mは、クロック入力端子４１５から制御パルスが１個入るごとに、それぞれ、セレクタ421_1～421_mの出力を保持して、保持している値を出力する。これらＤ型フロップフリップ422_1～422_mの出力は、ｍビット並列に、内部状態出力端子４１８から出力され、これらのうちのいくつかのビットが排他的論理和回路４１１（図５参照）に入力する。

【００１３】次に、各擬似乱数発生回路401_1～401_nの構成について説明する。擬似乱数発生回路401_1～401_nとしては、例えば、図７に示すように線形フィードバック・シフトレジスタのみで構成された擬似乱数発生回路５０１を使用することもできるし、図８に示すように非線形関数回路と線形フィードバック・シフトレジスタを組み合わせた擬似乱数発生回路５１１を使用することもできるし、さらにはここで述べるのとは異なる回路構成のものも使用することもできる。

【００１４】まず、図７を用いて線形フィードバック・シフトレジスタのみからなる擬似乱数発生回路５０１を説明する。この擬似乱数発生回路５０１は、シフトレジスタ５０２と排他的論理和回路５０３とから構成されている。シフトレジスタ５０２は、段数は異なっていてもよいが図６に示すシフトレジスタ４１０と同様の構造を持つものである。シフトレジスタ５０２のクロック入力端子、モード切り換え信号入力端子、内部状態入力端子（いずれも図６参照）は、それぞれ、入力端子４０５，４０６，４０７に接続している。そして、シフトレジスタ５０２の内部状態出力端子（図６参照）からの出力のうち予め決められたビットだけが排他的論理和回路５０３に供給され、排他的論理和回路５０３の出力が、出力端子５０４から出力されるとともに、シフトレジスタ５０２のシフト入力端子（図６）に供給されている。なお、排他的論理和回路５０３は、入力された各ビットのデータの排他的論理和を計算して、その結果を出力するものである。

【００１５】図７に示す擬似乱数発生回路５０１は、いわゆるＭ系列発生回路であり、この回路単独で発生させた擬似乱数のランダム性はあまり良くなく、また、初期状態を容易に推定することができるので、単独では暗号化のために使用することには適さない。

【００１６】図８に示す擬似乱数発生回路５１１は、シフトレジスタ５１２と排他的論理和回路５１３の他に、非線形関数回路５１４を有している。シフトレジスタ５１２は、段数は異なっていてもよいが図６に示すシフトレジスタ４１０と同様の構造を持つものである。シフトレジスタ５１２のクロック入力端子、モード切り換え信号入力端子、内部状態入力端子（いずれも図６参照）は、入力端子４０５，４０６，４０７に接続している。そして、シフトレジスタ５１２の内部状態出力端子（図６参照）からの出力のうち予め決められたビットが排他的論理和回路５１３に供給されて、排他的論理和回路５１３の出力がシフトレジスタ５１２のシフト入力端子（図６）に供給されている。なお、排他的論理和回路５１３は、入力された各ビットのデータの排他的論理和を計算して、その結果を出力するものである。さらに、シフトレジスタ５１２の内部状態出力端子からの出力の全ビットあるいは予め定められたビットが非線形関数回路５１４に入力して非線形結合され、この非線形結合された結果が擬似乱数として出力端子５１５から出力される。

【００１７】次に、結合関数について説明する。結合関数とは、既に述べたように、入力されたビットの非線形結合をとって、その結果を出力するものである。結合関数を出力する結合関数回路は、論理関数回路やリード・オンリ・メモリあるいはそれらの組合せによって実現できる。図９は３入力の結合関数回路４５０を示す機能ブロック図である。すなわちこの結合関数回路４５０は、図４や図５の擬似乱数発生装置においてＮ＝３（擬似乱数発生回路の数が３個）の場合に、結合関数回路４０２として使用できるものである。

【００１８】この結合関数回路は、否定回路４５１と、２つの２入力論理積回路４５２，４５３と、２入力排他的論理和回路４５４と、それぞれ異なる擬似乱数発生回路が発生する擬似乱数が入力する３個の入力端子455_1～455_3と、排他的論理和回路４５４の出力に接続された出力端子４５８とによって構成されている。第１の入力端子455_1に入力した擬似乱数は第１の論理積回路４５２の一方の入力に供給され、第２の入力端子455_2に入力した擬似乱数は第１の論理積回路４５２の他方の入力と否定回路４５１に供給される。第２の論理積回路４５３には、第３の入力端子455_3に入力した擬似乱数と、否定回路４５１で反転された第２の入力端子455_2からの擬似乱数が入力する。そして、各論理積回路４５２，４５３は、それぞれへの入力の論理積を計算して結果を排他的論理和回路４５４に出力し、排他的

論理和回路４５４は、第１の論理積回路４５２の出力と第２の論理積回路４５３の出力の排他的論理和を計算してその結果を出力端子４５８から出力する。

【００１９】

【発明が解決しようとする課題】以上、従来の擬似乱数発生装置についてやや詳しく説明したが、上述の従来の擬似乱数発生装置には、回路規模を小さくしようとすると非線形性の小さい擬似乱数しか生成できず、一方、非線形性の大きな擬似乱数を発生させようとすると装置規模が大きくなるという問題点がある。すなわち、回路規模を小さくするためには、擬似乱数発生回路として線形フィードバック・シフトレジスタのみからなるものを使用することが有効であるが、そうすると、非線形変換を行うのが結合関数回路だけとなり、非線形性の大きな擬似乱数を得ることができなくなる。また、回路規模を小さくするために擬似乱数発生回路の個数自体を減らした場合には、結合関数への入力数が減ることとなって結合関数の非線形性が小さくなり、非線形性がさらに小さな擬似乱数しか得られなくなる。逆に、得られる擬似乱数の非線形性を大きくするためには擬似乱数発生回路として非線形関数回路と線形フィードバック・シフトレジスタを組み合わせたものを用いることが有効であるが、そうすると、非線形関数回路を実現するための複雑な論理回路やリード・オンリ・メモリ（ＲＯＭ）が擬似乱数発生回路の個数だけ必要になってしまい、回路規模が必然的に大きくなる。また、擬似乱数の非線形性を大きくするために結合関数への入力数を増やすと、その分、擬似乱数発生回路の数も増やさなければならない。

【００２０】本発明の目的は、上述した従来の擬似乱数発生装置の抱える問題点を解決し、線形フィードバック・シフトレジスタのみからなる少数の擬似乱数発生回路によって非線形性の大きな擬似乱数系列を発生でき、ストリーム暗号に適した擬似乱数発生装置を提供することにある。

【００２１】

【課題を解決するための手段】本発明の第１の擬似乱数発生装置は、同一のクロックが入力し相互に同期して動作する複数の擬似乱数発生回路と、各擬似乱数発生回路の出力を非線形関数で結合して出力する結合関数回路と、クロックに同期して記憶内容を一端から他端に向う方向に１ビットずつシフトするとともに結合関数回路の出力を一端に記憶するシフトレジスタと、シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路とを有し、クロックに同期して非線形関数回路より擬似乱数を出力する。

【００２２】本発明の第２の擬似乱数発生装置は、同一のクロックが入力し相互に同期して動作する複数の擬似乱数発生回路と、各擬似乱数発生回路の出力を非線形関数で結合して出力する結合関数回路と、シフトレジスタと、シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路と、結合関数回路の出力と非線形関数回路の出力との排他的論理和を計算して出力する排他的論理和回路とを有し、シフトレジスタは、クロックに同期して記憶内容を一端から他端に向う方向に１ビットずつシフトするとともに排他的論理和回路の出力を一端に記憶し、擬似乱数がクロックに同期して非線形関数回路より出力される。

【００２３】本発明の第３の擬似乱数発生装置は、入力するクロックに同期して動作する単一の擬似乱数発生回路と、シフトレジスタと、シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路と、擬似乱数発生回路の出力と非線形関数回路の出力との排他的論理和を計算して出力する排他的論理和回路とを有し、シフトレジスタは、クロックに同期して記憶内容を一端から他端に向う方向に１ビットずつシフトするとともに排他的論理和回路の出力を一端に記憶し、擬似乱数がクロックに同期して非線形関数回路より出力される。

【００２４】本発明においては、擬似乱数発生回路として、線形フィードバック・シフトレジスタを好ましく使用できる。また、擬似乱数発生回路とシフトレジスタに初期値を設定する初期値設定回路を設けるようにするよい。さらに、結合関数回路の出力も非線形関数回路に入力し、非線形関数回路によって、シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値と結合関数回路の出力とが非線形結合して出力されるようにしてもよい。

【００２５】以下、本発明についてさらに詳しく説明する。

【００２６】図５に示す従来の擬似乱数発生装置では、結合関数回路４０２の出力系列をシフトレジスタ４１０に保持し、シフトレジスタ４１０の内部状態のすべてあるいは予め決められた一部のビットを排他的論理和回路４１１によって線形結合して擬似乱数を生成していた。このように構成すると、ある擬似乱数発生回路４０１$_j$（$1 \leqq j \leqq N$）の出力で条件付けたときの擬似乱数の条件付き確率分布がほぼ一様になるため、コリレーション・アタックが困難になる。このような手法は、物理的な方法で発生される乱数（例えば、サイコロを振って決められる乱数）の分布を一様にする目的でも、長年にわたって用いられてきた。このため、コリレーション・アタックを防ぐためには、線形結合が有用だと考えられていた。

【００２７】しかしながら、線形結合によって条件付き確率が一様になるのは、線形結合の線形性によるものではなく、線形結合の一様性によるものである。ここで、一様とは、ランダムに与えられたビットを結合することにより、ほぼ等確率に"０"と"１"を生ずることである。したがって、一様な非線形結合であれば、線形結合の代りに用いても、コリレーション・アタックを防ぐことが

可能なはずである。

【００２８】そこで本発明では、図５に示す従来の擬似乱数発生装置における排他的論理和回路の代りに、一様な非線形結合を行う非線形関数回路を使用し、結合関数回路の出力が入力するシフトレジスタの内部状態をこの非線形関数回路によって非線形結合して擬似乱数として出力する。このように構成することにより、コリレーション・アタックを防ぐという性質を保ったまま、擬似乱数の非線形性を高められる。さらに本発明では、結合関数回路とシフトレジスタとの間に排他的論理和回路を設け、非線形関数回路の出力と結合関数回路の出力を排他的論理和で足し込んだものがシフトレジスタに入力するように構成することができる。このように構成すると、非線形関数回路の出力がシフトレジスタにフィードバックされることになり、非線形関数回路で行われる非線形結合の非線形性が小さい場合であっても、ｘの２乗がx^2に、その２乗がx^4に、さらにその２乗がx^8にという具合に非線形性の低い変換の繰り返しが非線形性の高い変換に帰着することから、非線形性がさらに高められた擬似乱数を得ることが可能になる。

【００２９】

【発明の実施の形態】次に、本発明の実施の形態について、図面を参照して説明する。

【００３０】《第１の実施の形態》図１は、本発明の第１の実施の形態の擬似乱数発生装置の構成を示す機能ブロック図である。この擬似乱数発生装置は、ｎ個の擬似乱数発生回路１０１$_1$～１０１$_n$と、これらｎ個の擬似乱数発生回路１０１$_1$～１０１$_n$の出力を非線形結合してその結果を出力する結合関数回路１０２と、結合関数回路１０２の出力がシフト入力として入力するシフトレジスタ１０３と、シフトレジスタ１０３の内部状態のうち予め定められた複数のビット（シフトレジスタ１０３の全記憶ビットでもよい）の非線形結合を計算する非線形関数回路１０４と、制御パルス（クロック）が入力する入力端子１０５と、モード制御用の入力端子１０６と、初期状態と呼ばれるビット系列を入力するための入力端子１０７とを有し、非線形関数回路１０４での計算結果が擬似乱数を表わすビットストリームとしてクロックに同期して出力端子１０８から出力されるように構成されている。なお、図示点線で示されるように、結合関数回路１０２の出力も非線形関数回路１０４に入力するようにしてもよい。

【００３１】ｎ個の擬似乱数発生回路１０１$_1$～１０１$_n$は、いずれも、入力端子１０５～１０７に接続しており、入力端子１０６に"０"が供給されている時に入力端子１０５に制御パルスが入力された場合には、入力端子１０７から供給される初期状態を取り込んで内部状態として保持し、入力端子１０６に"１"が供給されている場合には、入力端子１０５に制御パルスが１個入力されるごとに擬似乱数を出力する。この擬似乱数発生回路１０１$_1$～１０１$_n$としては、上述の図７に示したような線形フィードバック・シフトレジスタのみからなるものを好ましく使用できる。また、シフトレジスタ１０４は、入力端子１０５～１０７にも接続しており、入力端子１０６に"０"が供給されている時に入力端子１０５に制御パルスが入力すると、入力端子１０７から供給されている初期状態と呼ばれるビット系列を内部状態として保持し、入力端子１０６に"１"が供給されている場合には、入力端子５０５に制御パルスが１個入力されるごとに、内部状態を１ビットだけ右にシフトし、左端のビットに結合関数回路１０２の出力を保持するように構成されている。シフトレジスタ１０４としては、例えば、上述の図６に示す構成のものを使用することができる。

【００３２】上述の説明から明らかなように、擬似乱数発生回路１０１$_1$～１０１$_n$、結合関数回路１０２、入力端子１０５～１０７は、それぞれ、図４及び図５における擬似乱数発生回路４０１$_1$～４０１$_n$、結合関数回路４０２、入力端子４０５～４０７に対応し、シフトレジスタ１０３は、図５のシフトレジスタ４１０に対応する。また、結合関数回路１０２と非線形関数回路１０４は、この分野での慣例に従って別の名称で呼んでいるが、どちらも非線形結合を行う回路であるという点では同様のものである（入力ビット数や内部構造は異なるかもしれないが）。

【００３３】非線形関数回路１０４としては、一様な非線形結合を行う回路であれば任意のものを使用できる。例えば、リード・オンリ・メモリ（ＲＯＭ）を用いたルック・アップ・テーブル形式の構成とすることができる。具体的には、図１０(a)に示すように、ＲＯＭ１５１に"０"と"１"とを個数が等しくなるように書き込んでおき、非線形関数回路１０４に対する複数の入力をこのＲＯＭ１５１の複数のアドレス入力端子それぞれへのアドレス入力とみて、このＲＯＭ１５１からの１ビットのデータ出力を非線形関数回路１０４の出力とするような構成とすることができる。非線形関数回路１０４の入力数、すなわちＲＯＭに対する入力ビット数が増えた場合には、１個のＲＯＭを用いたのでは実現できなくなるが、そのような場合には、図１０(b)に示すように、上述したＲＯＭ１５１を複数用意してこれらＲＯＭ１５１の出力を排他的論理和回路１５２に入力し、この排他的論理和回路１５２の出力を非線形関数回路１０４の出力とするように構成すればよい。

【００３４】なお、擬似乱数発生回路１０１$_1$～１０１$_n$及びシフトレジスタ１０３には、入力端子１０７を介して一般に、それぞれ異なる初期状態が供給される。各擬似乱数発生回路１０１$_1$～１０１$_n$やシフトレジスタ１０３に供給される初期状態は、それぞれ、それらの内部ビット幅に応じて複数のビットであるから、入力端子１０７のビット幅は、これら擬似乱数発生回路１０１$_1$～１０１$_n$やシフトレジスタ１０３の内部ビット幅の総和と

なるようにするとよい。あるいは、内部状態設定のための制御が個別に行えるような構成とするとよい。図示した例では、各擬似乱数発生回路１０１$_1$～１０１$_n$及びシフトレジスタ１０３に初期状態のビット系列を設定するために、入力端子１０７に、これら擬似乱数発生回路１０１$_1$～１０１$_n$やシフトレジスタ１０３の初期状態を発生する初期状態設定回路１１０が接続されている。

【００３５】この擬似乱数発生装置を用いて擬似乱数を発生させる場合には、まず、擬似乱数発生回路１０１$_1$～１０１$_n$及びシフトレジスタ１０３の初期状態を初期値設定回路１１０によって入力端子１０７に供給する。次いで、入力端子１０６に"０"を供給して入力端子１０５に制御パルスを１個入力する。その結果、各擬似乱数発生回路１０１$_1$～１０１$_n$及びシフトレジスタ１０３に初期状態が設定される。そして、入力端子１０６に"１"を供給すると、それ以降は、入力端子１０５に制御パルスを１個入力するごとに、出力端子１０８から１ビットずつ擬似乱数が得られる。

【００３６】《第２の実施の形態》次に、本発明の第２の実施の形態について、図２を用いて説明する。図２に示す擬似乱数発生装置は、図１に示すものと比べ、結合関数回路１０２とシフトレジスタ１０３との間に排他的論理和回路１１１が挿入され、シフトレジスタ１０３のシフト入力には、結合関数回路１０２の出力ではなく排他的論理和回路１１１の出力が入力する点で異なっている。排他的論理和回路１１１は、結合関数回路１０２の出力と非線形関数回路１０４の出力との排他的論理和を求めて出力する。この擬似乱数発生装置では、排他的論理和回路１１１を介して非線形関数回路１０４の出力がシフトレジスタ１０３にフィードバックされるので、非線形関数回路１０４の非線形性が小さい場合であっても、非線形性の大きな擬似乱数を出力端子１０８から得ることができる。この擬似乱数発生装置を用いて擬似乱数を発生させるときの手順は、図１に示す擬似乱数発生装置での手順と同じである。

【００３７】《第３の実施の形態》上述の各実施の形態の擬似乱数発生装置は、出力端子１０８に接続する非線形関数回路１０４によって非線形性を高めているので、特に第２の実施の形態のように非線形関数回路１０４の出力をシフトレジスタ１０３にフィードバックさせる場合には、擬似乱数発生回路の個数を１個としても、十分に非線形性の高い擬似乱数を得ることができる。図３は、このような構成の擬似乱数発生装置を示している。この擬似乱数発生装置では、単一の擬似乱数発生回路１０１が設けられている。擬似乱数発生回路が１個なので結合関数回路は不要であり、この擬似乱数発生回路１０１の出力がそのまま排他的論理和回路１１１に入力している。その他の構成や擬似乱数発生のための手順は第２の実施の形態におけるものと同様である。

【００３８】【発明の効果】以上説明したように本発明は、ある擬似乱数発生回路の出力で条件付けたときの擬似乱数の条件付き確率分布を一様にするために、線形結合回路でなく一様な非線形結合を行う非線形関数回路を使用しているので、擬似乱数の非線形性が高められ、コリレーション・アタックに強い擬似乱数を発生でき、ストリーム暗号に適した擬似乱数発生装置が実現できるという効果がある。また、擬似乱数発生回路として単純な線形フィードバック・シフトレジスタを使用しても擬似乱数の非線形性が高いので、小規模な装置で非線形性の高い擬似乱数を発生できるようになり、擬似乱数発生装置を低コストで実現できるようになる。

【００３９】また、非線形関数回路の出力が排他的論理和回路を介してシフトレジスタにフィードバックするように構成した場合には、非線形変換の繰返しが行われることになって、非線形関数回路の非線形性が小さい場合でも非線形性のより大きな擬似乱数を生成できるようになり、したがって、非線形関数回路の規模を小さくすることができるようになる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の擬似乱数発生装置の構成を示す機能ブロック図である。

【図２】本発明の第２の実施の形態の擬似乱数発生装置の構成を示す機能ブロック図である。

【図３】本発明の第３の実施の形態の擬似乱数発生装置の構成を示す機能ブロック図である。

【図４】従来の擬似乱数発生装置の一例を示す機能ブロック図である。

【図５】コリレーション・アタック対策の施された従来の擬似乱数発生装置の一例を示す機能ブロック図である。

【図６】シフトレジスタの構成例を示す回路図である。

【図７】線形フィードバック・シフトレジスタを利用した擬似乱数発生回路を示す機能ブロック図である。

【図８】非線形関数回路と線形フィードバック・シフトレジスタを利用した擬似乱数発生回路を示す機能ブロック図である。

【図９】３入力の結合関数回路を示す回路図である。

【図１０】(a),(b)は、それぞれ、非線形関数回路の構成例を示す回路図である。

【符号の説明】

１０１,１０１$_1$～１０１$_n$,４０１$_1$～４０１$_n$　擬似乱数発生回路

１０２,４０２,４５０　結合関数回路

１０３,４０３,４１０,５０２,５１２　シフトレジスタ

１０４,５１４　非線形関数回路

１０５～１０７,４０５～４０７　入力端子

１０８,４０８　出力端子

１１０　初期値発生回路

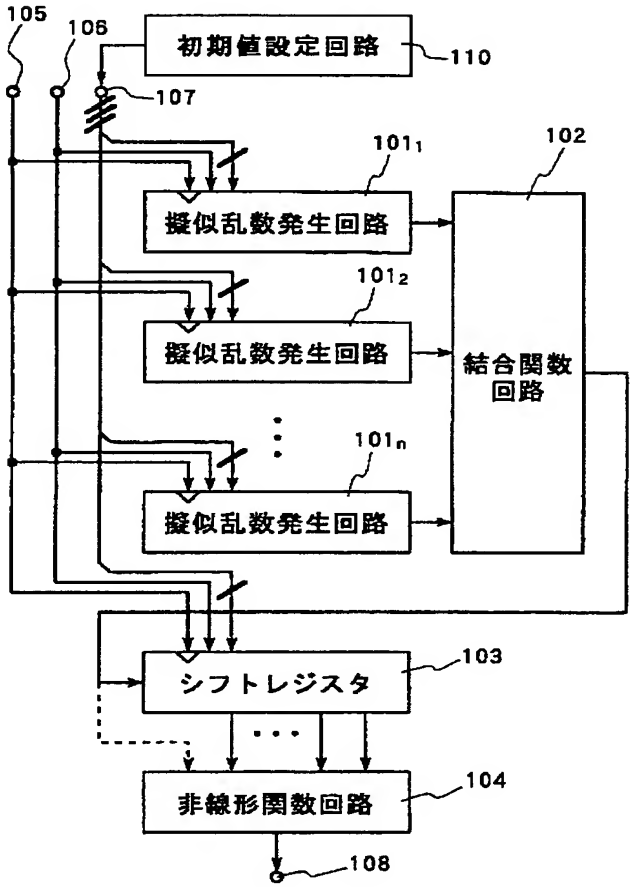
13

１５１　　ＲＯＭ
１１１，１５２，４１１，４５４，５０３，５１３　　排他的論理和回路
４１５　　クロック入力端子
４１６　　モード切り換え信号入力端子
４１７　　内部状態入力端子

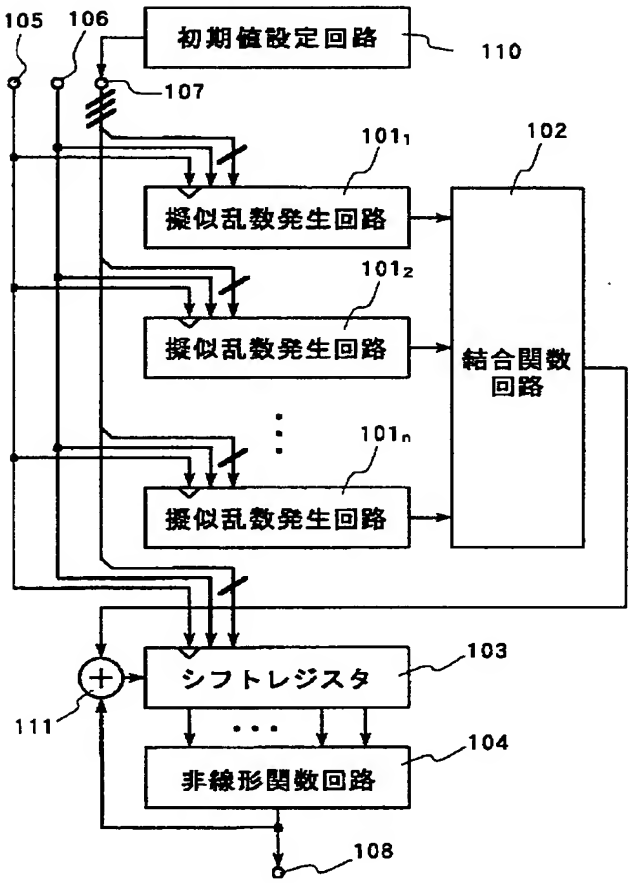
14

４１８　　内部状態出力端子
４１９　　シフト入力端子
421_1～421_m　　セレクタ
422_1～422_m　　Ｄ型フリップフロップ
４５１　　否定回路
４５３，４５３　　論理積回路

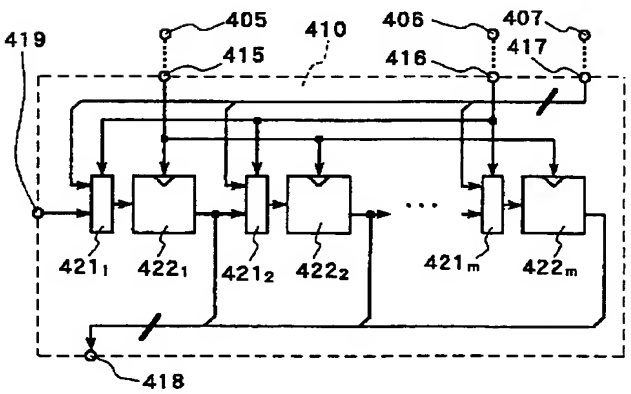
【図１】



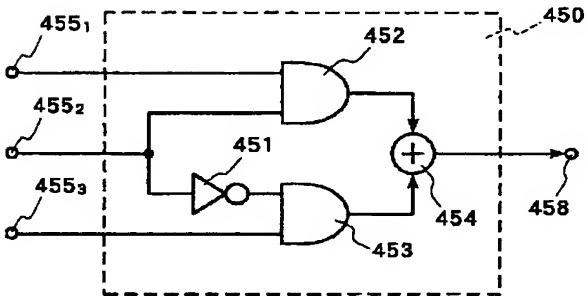
【図２】



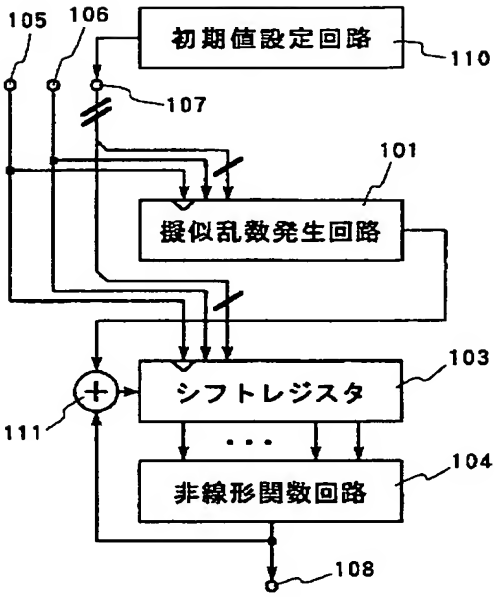
【図６】



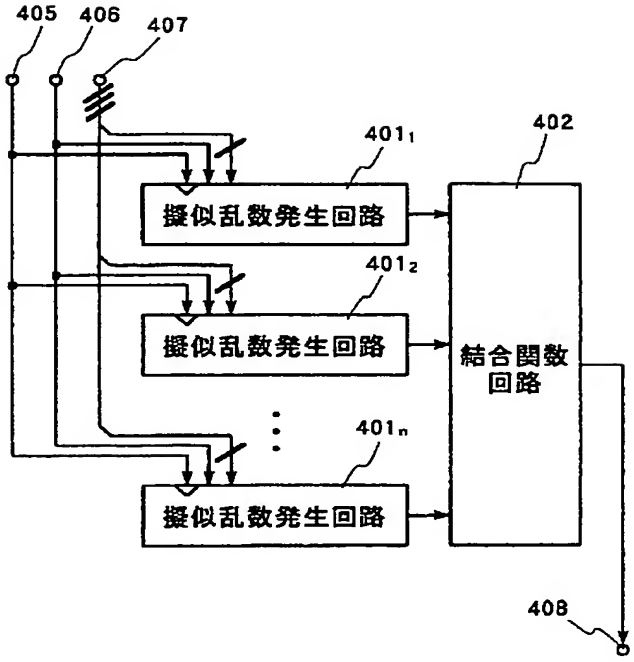
【図９】



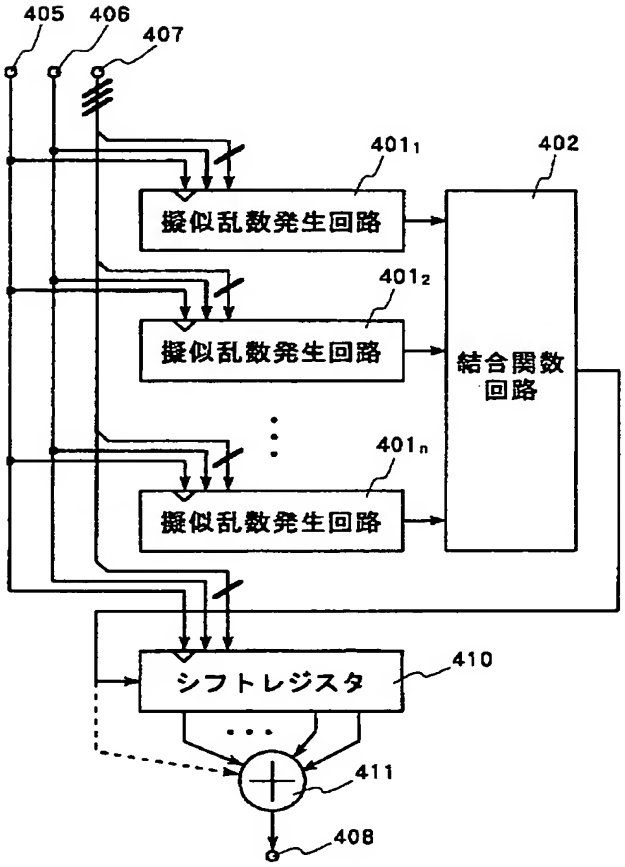
【図３】


105
106
初期値設定回路
110
107
101
擬似乱数発生回路
103
シフトレジスタ
111
104
非線形関数回路
108

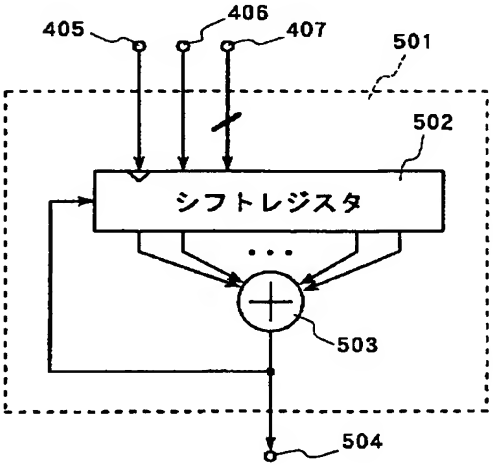
【図４】


405
406
407
401₁
402
擬似乱数発生回路
401₂
擬似乱数発生回路
結合関数回路
401n
擬似乱数発生回路
408

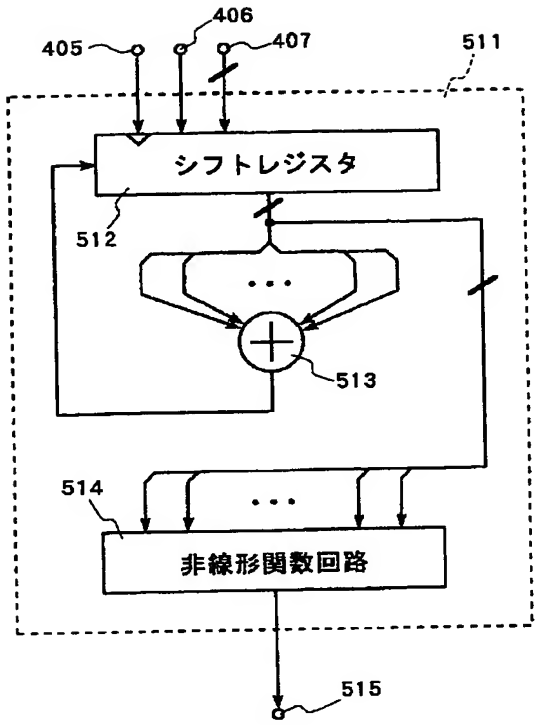
【図５】


405
406
407
401₁
402
擬似乱数発生回路
401₂
擬似乱数発生回路
結合関数回路
401n
擬似乱数発生回路
410
シフトレジスタ
411
408

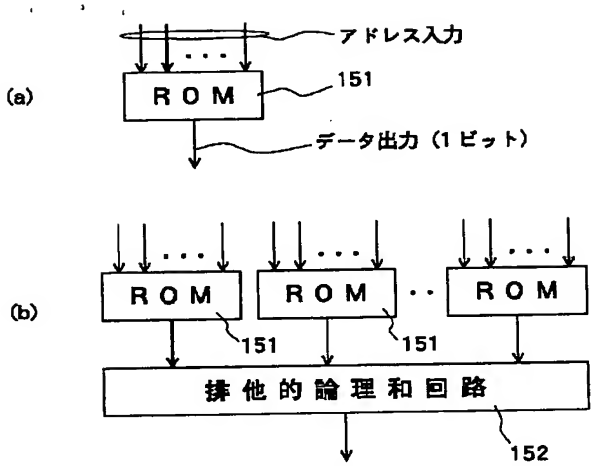
【図７】


405
406
407
501
502
シフトレジスタ
503
504

【図８】


406
405
407
511
シフトレジスタ
512
513
514
非線形関数回路
515

【図１０】


(a)
アドレス入力
ROM
151
データ出力（1ビット）
(b)
ROM
ROM
ROM
151
151
排他的論理和回路
152